UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/441,403	11/16/1999	Benjamin Hewitt Smith	BSIL-110CP	4276

7590 04/21/2004

Mark G Lappin
McDermott Will & Emery
28 State Street
BOSTON, MA 02109

EXAMINER	
KLIMACH, PAULA W	
ART UNIT	**PAPER NUMBER**
2135	10

DATE MAILED: 04/21/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/441,403	SMITH ET AL.	
	Examiner	Art Unit	
	Paula W Klimach	2135	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *02 February 2004*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-59* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-59* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date 4/5
4) ☒ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

Response to Amendment

This office action is in response to amendment filed on 2/2/04 (Paper No. 9). Original application contained Claims 1-59. The amendment filed on 2/2/04 have been entered and made of record. Therefore, presently pending claims are 1-59.

Response to Arguments

Applicant's arguments filed 2/2/04 have been fully considered but they are not persuasive because of following reasons.

Applicant argued that claims 1, 20, 29, 38, 57, and 58 define a system that establishes or installs a network among linked nodes. This is not found persuasive. The office calls attention to the limitation B, "an installation server, configured to facilitate installation of said at least one software application." The office therefore asserts that the applicant claims an installation server that installs software to the network that enables the nodes in the network to communicate with each other in a secure network. Further reasons are specified in the new grounds of rejection as set forth below.

Applicants clearly have failed to explicitly identify specific claim limitations, which would define a patentable distinction over prior arts. The examiner is not trying to teach the invention but is merely trying to interpret the claim language in its broadest and reasonable meaning. The examiner will not interpret to read narrowly the claim language to read exactly from the specification, but will interpret the claim language in the broadest reasonable interpretation in view of the specification. Therefore, the examiner asserts that the prior art does teach or suggest the subject matter broadly recited in independent Claims 1, 20, 29, 38, 57, and

58. Dependent Claims 2-19, 21-28, 30-37, and 39-56 are also rejected at least by virtue of their dependency on independent claims and by other reason set forth in this office action (Paper No. 10). Accordingly, rejections for claims 1-59 are respectfully maintained.

Specification

1. The title of the invention is not descriptive. A new title is required that is clearly indicative of the invention to which the claims are directed.

The following title is suggested: Remote software installation for enabling node communication on a network.

2. The disclosure is objected to because of the following informalities:

The lengthy specification has not been checked to the extent necessary to determine the presence of all possible minor errors. Applicant's cooperation is requested in correcting any errors of which applicant may become aware in the specification.

Claim Objections

3. Claim objection is withdrawn

Claim Rejections - 35 USC § 103

4. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

5. **Claims 1-12, 16, 20, 29-34, 38-47, 53, 57, 58** are rejected under 35 U.S.C. 103(a) as being unpatentable over Shostack et al (6,298,445) in view of Sandahl (6,098,098).

In reference to claims 1, 20, 29, and 38, Shostack discloses installing software and updates to a plurality of linked remote computers (Fig. 1), and monitoring a secure network of nodes (Fig. 2), said system comprising: at least one software application (column 2 lines 35-38 in combination with column 8 lines 12-15); an installation server, configured to facilitate installation of said at least one software application (column 8 lines 1-18). In reference to the generator, configured to generate a plurality of software components from a network definition. The push mechanism carries out the functionality of the generator by delivering the software enhancement to the customer therefore it generates the plurality of components from the network definition (software upgrade) for delivery to the client computer (column 8 lines 42-54). The node agent modules are embodied in the Shostack system by the pull mechanism in the client that initiates communication with the server and the subsequent installation of the software on the client which is the remote computer and forms the node (column 9 lines 25-37). The Shostack system includes a monitor node configured to monitor security of said network (column 7 lines 20-27). The push system generates the components for the update and the software installation from the data provided by the NSD (Network security Detector, column 7 lines 15-19). The NSD defines system by defining the vulnerabilities in the system and adds these to the database, which the push system uses to create the updates for the security software.

Shostack does not expressly disclose the plurality of nodes each of capable of automatically establishing communication with others of said nodes according to said network definition.

Sandahl discloses a system wherein managed devices receive master files form the server, therefore they receive the network definition (configuration) from the server. The managed devices then use the information in the files to connect to the network and communicate with other nodes (column 3 lines 14-25).

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to use the installation server as in Shostack to download the network definition (configuration) as in Sandahl. One of ordinary skill in the art would have been motivated to do this because it would improve the control over the network of the configuration of devices to provide desired network system operation.

In reference to claims 2-3, wherein the remote computers are linked substantially by the Internet and the intranet (Shostack column 4 lines 13-21). The system is a local network (intranet) that is connected to the Internet.

In reference to claims 4-5, and 39, Shostack system authenticates the identity of the user and the integrity of the connection (column 13 lines 31-36) as a result the system would inherently have to identify one of said plurality of remote computers to obtain the integrity of the computer; an identification of at least one software application to be installed on said remote computer to form a node (Fig. 4B); and an identification of each other node to which said node is to be linked to, and the remote computers IP address and node name to define the map of all ports on the network as describe in column 7 lines 17-18.

In reference to claim 7, 32-33, 41, and 44, the installation server of Shostack is configured to facilitate said installation of said corresponding software application as a function

of a verification that said agent module is executing on said corresponding remote computer, according to said network definition (column 4 lines 22-27).

In reference to claims 8, 30, 31, and 43, the installation server of Shostack is configured to facilitate said installation of said corresponding software application as a function of a verification that said agent module has not been previously installed (column 9 lines 25-30 in combination with column 10 lines 50-55).

In reference to claim 9, the firewall is the second node of Shostack is configured to determine the presence of an interposed, unintended node (column 6 lines 35-40). The firewall is the first line of defense and therefore detects the unintended node attempting to connect to the network.

In reference to claim 10, the monitor node is further configured to selectively terminate operation and connection of one or more tainted nodes in response to a detected security violation (Shostack column 6 lines 57-58).

In reference to claims 11 and 46-47, the system initiates a regeneration of a set of said software components (column 11 lines 50-51), reinstallation of said at least one software application (the update processor implements the suggested repairs and therefore a new installation, column 11 lines 51-54), and selective relinking to other nodes for each of said selectively terminated one or more tainted nodes and according to said network definition (the intruder is disengaged therefore the nodes that the intruder has connected to and as a result there is a selective linking which leaves out the nodes that have been violated, column 6 lines 57-58).

In reference to claim 12, the monitor node and each of said nodes communicate using secure data transfer using an asymmetric cryptosystem (Shostack column 13 lines 55-65).

In reference to claims 16 and 53, further Shostack includes the monitor generating a report that is sent to the management station for analysis (column 13 lines 23-27) where accounts may be analyzed and therefore generate billing information as a function of the selective linking of said node to said other nodes.

In reference to claim 34, Shostack teaches a system that is configured to analyze software components and determine the presence of trap doors (Table 1).

In reference to claims 42 and 45, the system disclosed by Shostack suggests generating a unique local password for each node and verifies the remote computer by entering the local password and verifying the local password (Table 1).

In reference to claims 57 and 58, Shostack discloses a system for generating a install process to a plurality of remote computers, and monitoring a secure network having a plurality of nodes, a generator, an installation server, and a monitor node (column 4 lines 13-21), said network may be used for conducting financially related transactions between a custody system of a bank and a trading system of a financial client because they require secure communications of data as suggested by Shostack. The system created by Shostack modifies often depending on vulnerabilities (column 4 lines 47-50), and could be used by a bank sales department, which creates a network definition embodying the network required by the financial client and to be generated, installed and monitored by the bank owning the network security detection system as in Shostack. Modeling and testing said network definition, by a bank development group, which would use the network security detection for testing the system as disclosed by Shostack (column 7 lines 20-30) and then initiate the updates (column 9 lines 25-27). Obtaining authorization from a bank network administration group and installing said network definition on said generator, by

said bank development group (column 9 lines 25-27). Obtaining by said bank sales group a sales password and authorization to install network from said network administration group, suggested by Table 1, which shows that passwords are used for authorization and therefore examined for vulnerabilities. Shostack suggests auditing on said generator a generated network definition by comparing said generated network definition to said network definition and inputting said sales password as an indication of a favorable comparison, by said bank sales group. Since the system checks the file to see if it is the most current file before installing it, the network is defined by the vulnerabilities of the network, where the most resent vulnerabilities would be contained in the most resent install which is the most recent network definition (column 10 lines 50-55). The password of the sales and audit group are common methods of verifying the user is eligible for the software enhancement (column 8 lines 22-25). The system generates with said generator a plurality of software components to be installed on said plurality of remote computers to form said plurality of nodes of said network, said components including: (i) a plurality of agent modules, each agent module having the capability to establish communications with said installation server; (ii) a local sales password, for each agent module; (iii) a local audit password for each agent module (column 13 lines 1-7 in combination with lines 47-50). Registering said agent modules with said installation server, wherein said installation server has access to at least one or more bank custody software applications to be stored on each of said plurality of remote computers to form said nodes, according to said network definition. The remote device connects to the network service thereby giving information about itself, and thus registering (column 12 lines 58-61). Communicating to each remote computer a corresponding one of said local sales passwords to a sales department representative, and communicating to each remote computer a

corresponding one of said local audit passwords to an audit department representative is suggested in the system by Shostack because of the use of passwords (column 12 lines 58-61). Executing each agent module on its corresponding remote computer, entering said local sales password to verify that said agent module is installed on its corresponding remote computer according to said network definition, and downloading said corresponding at least one bank custody software application (column 8 lines 7-18 in combination with column 10 lines 42-49). Executing each of said at least one software applications on its corresponding remote computer, establishing communication with said monitor node entering said local audit password to verify that said at least one software application is installed on its corresponding remote computer according to said network definition (column 12 lines 47-57). The system checks that map network and programs therefore verifying the software application is installed on its corresponding remote computer according to the network definition. Selectively linking said nodes into said network is suggested in column 6 lines 56-58, since nodes can be electronically disconnected.

Shostack does not expressly disclose the plurality of nodes each of capable of automatically establishing communication with others of said nodes according to said network definition.

Sandahl discloses a system wherein managed devices receive master files form the server, therefore they receive the network definition (configuration) from the server. The managed devices then use the information in the files to connect to the network and communicate with other nodes (column 3 lines 14-25).

In reference to claims 6 and 40, Shostack does not disclose a plurality of node configuration files, wherein a different one of said node configuration files corresponds to a different node and includes information for facilitating selective communication with others of said nodes according to said network definition; and at least one network information file, having information corresponding to substantially all links between nodes and accessible by said monitor node to facilitate the selective linking of said nodes.

Sandahl discloses a system for managing the configuration of multiple computer devices over a network (column 2 lines 27-34). The system includes a file server that has memory for storing master configuration information for each of the computer devices on the network, and the computer device compares data characterizing its master configuration information with its local configuration. This means that each computer keeps a copy of its local configuration (column 2 line 56 to column 3 line 5).

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to use a file server to maintain copies configuration information as taught by Sandahl in the system disclosed by Shostack. One of ordinary skill in the art would have been motivated to do this because it would assure that the configuration of each network device provides desired network system operation while minimizing network bandwidth usage (Sandahl column 2 lines 20-25).

Claim Rejections - 35 USC § 103

6. **Claims 13-15, 17-19, 21-28, 35-37, 48-52, 54-56, and 59** are rejected under 35 U.S.C. 103(a) as being unpatentable over Shostack and Sandahl as applied to claim 12, 1, and 38 respectively above, and further in view of Schneier.

In reference to claims 13, 17, 21, 25, 26, 35, 48, and 55, Shostack discloses each sender having a unique key (column 14 lines 17-18).

However Shostack does not expressly disclose a system wherein said secure data transfer is accomplished using data encryption, and wherein data transferred in each direction between two linked nodes is encrypted differently.

Schneier discloses the use of encryption for two-party communication (Figure 1.3). The data transferred in each direction between two linked nodes is encrypted differently because each end nodes has a different key because there is only one private key for decryption and the public key is published for encryption, therefore each party would publish their specific public key and the data would therefore be encrypted differently.

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to use encryption to send data from one node to another as described in Schneier. One of ordinary skill in the art would have been motivated to do this because encryption is used to disguise a message in such a way as to hide its substance (Schneier page 1 paragraph 2).

In reference to claims 14, 23, and 54, each of two linked nodes uses a unique pair of encryption keys to accomplish said data encryption, and each pair of encryption keys includes a substantially hidden private key and a public key (Figure 1.3).

In reference to claims 15, 24, and 49-50, 52, the monitor node would have to selectively initiate a coordinated strobing of each pair encryption keys between two linked nodes to the unique key for every node.

In reference to claims 18, 22, 27, 36 and 51, Schneier teaches that a randomly generated private key and public key pair for data encryption (Figure 1.3), wherein data to be transferred to

said installation server is encrypted using said public key and is decrypted by said installation server using said private key (Figure 1.3). Schneier teaches that good keys are random-bit strings generated by some automatic process (page 173 paragraph 3).

In reference to claims 19, 28, 37, 56, the Shostack monitor node is configured to compare the installation server cryptographic checksum with the cryptographic checksum used by one of said plurality of remote computers to encrypt data sent to said installation server, a negative comparison being indicative of a security violation (Shostack, column 14 lines 21-29). After the comparison it would be elementary to signal a violation if the values do not match.

In reference to claim 59, it is inherit that financial data requires confidentiality. Therefore the first system of said first group is a custody system of a bank and said second system of said second group is a trading system of a financial services group, in the two party confidential communication (Figure 1.3).

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Paula W Klimach whose telephone number is (703) 305-8421. The examiner can normally be reached on Mon to Thr 9:30 a.m to 5:30 p.m.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on (703) 305-4393. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

PWK
Monday, April 19, 2004